Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de ATI (Asociación de Técnicos de Informática). _Novática_ edita también _Upgrade_, revista digital de CEPIS (_Council of European Professional Informatics Societies_), en lengua inglesa.

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro de CEPIS (*Council of European Professional Informatics Societies*) y tiene un acuerdo de colaboración con ACM (*Association for Computing Machinery*). Tiene asimismo acuerdos de vinculación o colaboración con AdaSpain, AI2 y ASTIC

Coordinación Editorial y Redacción Central (ATI Madrid)
Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica@ati.es*>
Composición, Edición y Redacción ATI Valencia
Reino de Valencia 23, 46005 Valencia
Tlf./fax 963330392 <*secreval@ati.es*>
Administración y Redacción ATI Cataluña
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlf.934125235; fax 934127713 <*secregen@ati.es*>
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel, Isla Cartuja 41092 Sevilla
Tlf./fax 954460779 <*secreand@ati.es*>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza
Tlf./fax 976235181 <*secreara@ati.es*>
Redacción ATI Asturias-Cantabria <*gp-astucant@ati.es*>
Redacción ATI Castilla-La Mancha <*gp-clmancha@ati.es*>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlf.986581413; fax 986580162 <*secregal@ati.es*>
Suscripción y Ventas: <*http://www.ati.es/novatica/interes.html*>, o en ATI Cataluña y ATI Madrid
Publicidad: Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica.publicidad@ati.es*>

Imprenta: 9·Impressió S.A., Juan de Austria 66, 08005 Barcelona.
Depósito Legal: B 15.154-1975
ISSN: 0211-2124; CODEN NOVAEC

Portada: Antonio Crespo Foix / © ATI 2003

novática
UPGRADE
Revista de la Asociación de Técnicos de Informática

MAYO · JUNIO 2003
163

SUMARIO

Monografía del próximo número:
«Ingeniería del Software: estado de un arte»

Seguridad

Ocultación de imágenes mediante Esteganografía

David Atauri Mezquida[1], Luis Fernández Sanz[1], Matías Alcojor[2], Ignacio Acero[3]
[1] Dpto. de Programación e Ingeniería del Software, Universidad Europea CEES; [2] Safo Sistemas; [3] Alma Technologies

<{atauri, lufern}@dpris.esi.uem.es>
<alcojor@safo.es>
<nachoa@airtel.net>

Resumen: *gracias a las técnicas de esteganografía podemos ocultar un fichero en otro y así enviarlo o distribuirlo sin que sea advertido. En este artículo se describe el algoritmo que inserta una imagen en formato BMP indexado dentro de otra imagen del mismo tipo. Por último, se hace una breve indicación de nuevas aplicaciones y de las implicaciones prácticas de esta tecnología.*

Palabras clave: *BMP, Esteganografía, formatos gráficos, ocultación de información.*

1. Introducción

La esteganografía es el arte de esconder mensajes y así hacerlos pasar inadvertidos para quien no conoce la manera de desvelarlos. Ejemplo remoto e inocente es el acróstico de la Celestina, donde se oculta el nombre de su autor y su lugar de nacimiento: «*Fernando de Roias acabo la comedia de Calysto y Melybea y fve nascido en la pvebla de Montalvan*» (ver **anexo**). Utilizada de forma artesanal durante muchos siglos, fue ampliamente utilizada en el siglo XX como ayuda en el espionaje, principalmente para transmitir información durante la Guerra Fría.

Lejos de ser cosa del pasado, hoy está de rabiosa actualidad. De hecho, algunas informaciones aparecidas en el diario U.S. Today sugerían (aunque no sin controversia por parte de los expertos) que podía haber sido utilizada por Bin Laden para organizar el atentado de las Torres Gemelas del 11 de septiembre de 2001, pasando a sus comandos información escondida en imágenes de Internet, en foros de noticias o en los mensajes de correo electrónico (véase [1] [2] [3]y [4]).

Todos hemos escrito, de niños, mensajes invisibles con jugo de limón que luego desvelábamos con la llama de un mechero. Otro método clásico y sencillo de esteganografía es pintar diminutos puntos bajo ciertas letras de una carta aparentemente inocua: esas letras son las que forman el mensaje oculto. La evolución ha llevado a métodos, típicos de película de espías, que consisten, por ejemplo, en miniaturizar el documento que se quiere ocultar de forma que parezca el punto final de una frase en una carta cualquiera.

Evidentemente, la aplicación de las nuevas tecnologías de la información ha supuesto una gran contribución a la evolución de las técnicas esteganográficas. En este artículo, veremos algunas aplicaciones sencillas de la esteganografía en ficheros electrónicos.

2. Definición y fundamentos

Podemos definir la esteganografía como el conjunto de técnicas que nos permiten ocultar cualquier tipo de información. No hay que confundir la criptografía con la esteganografía: la primera modifica los datos para hacerlos incomprensibles, mientras que la segunda simplemente los oculta entre otros datos. A pesar del diferente enfoque de cada una, en muchas ocasiones se combinan ambas técnicas para lograr mejores resultados.

Las razones para el uso de la esteganografía pueden ser muy variadas pero pueden aparecer porque no existe soporte para encriptar los datos o porque existe una autoridad que no permite el paso de cierta información. Así, la información viaja en los ficheros sin que nadie sepa lo que realmente transporta en su interior. Una de las aplicaciones de la esteganografía que actualmente más interés está suscitando es la aplicación de 'marcas de agua'(*watermarking*), que supongan un aviso de *copyright* o *trademark* oculto en imágenes, música o software comercial. Por otra parte, desde nuestro punto de vista, algunas de las técnicas de ocultación de virus en ficheros se pueden considerar en rigor como técnicas esteganográficas de ocultación del código maligno frente al usuario o, incluso, frente a programas antivirus.

La llegada de la informática ha permitido lograr grandes avances en las posibilidades de la esteganografía, consiguiéndose además automatizar tareas que solían ser bastante costosas en tiempo y dinero. El tipo de información que se puede ahora ocultar no se reduce a mensajes escritos; podemos ocultar digitalmente tanto texto e imágenes como sonido o incluso programas ejecutables (caso de los virus informáticos).

La base de la esteganografía informatizada se basa en que toda información digitalizada se reduce a cadenas de bits: dichas cadenas se pueden insertar ocultas entre los bits de otros ficheros que sirven de soporte o contenedor y que mantienen un aspecto inalterado. En general, se aprovecha el espacio de los bytes de basura que tienen los formatos conocidos de ficheros y, también, la información redundante. Así, si usamos archivos de sonido, la información oculta aparece como ruido de fondo, pudiendo confundirse fácilmente con una simple grabación con algo de ruido.

De hecho, cuando se esteganografía algo en un fichero binario, lo que se hace es ocultar la información en ficheros

como imágenes, en los que se pueden cambiar ciertos bits sin dejarlos inservibles. Por ejemplo, si queremos ocultar una cadena de ocho bits, cambiamos los bits menos significativos de los ocho primeros bytes del mapa de bits de una imagen en escala de grises (en el que cada pixel se corresponde con un byte) por los bits que queremos ocultar. El cambio en la imagen será tan pequeño que el ojo humano no captará la diferencia.

Para comprender mejor la aplicación de la esteganografía, en este artículo mostraremos un sencillo algoritmo de creación propia para esconder una imagen en blanco y negro dentro de otra imagen de color que no se ve aparentemente alterada. Pero antes comenzaremos por repasar los fundamentos del formato gráfico BMP que ha sido el elegido como base de nuestra demostración esteganográfica. En internet existen multitud de aplicaciones que utilizan otros formatos com JPEG, GIF ó PCX (por ejemplo, en <http://personal1.iddeo.es/albertoaa/steganos.htm> se pueden encontrar enlaces a varios de ellos).

3. El formato BMP

BMP es un formato gráfico creado por Microsoft para Windows [5]. Permite grabar imágenes de diferentes profundidades de bit o cantidad de colores. A continuación veremos el formato de 8 bits por pixel. Para su estudio utilizaremos un editor hexadecimal con el que podremos leer el fichero byte a byte. Cada byte puede almacenar un número entre 0 y 255 que se representa en un editor hexadecimal con 2 cifras (de 00 a FF).

Aunque BMP puede utilizar compresión RLE nos fijaremos en el caso de una imagen grabada sin compresión por mayor simplicidad.

El formato BMP de 8 bits por píxel puede representar 256 colores diferentes y es de tipo indexado. Esto quiere decir que los 256 colores disponibles para la imagen se almacenan en una tabla o paleta de colores que es exclusiva de dicha imagen. Dos imágenes diferentes tendrán por lo tanto dos paletas diferentes.

En el formato de fichero se distinguen los bloques que se explican a continuación.

3.1. Cabecera

Contiene información relativa al fichero pero no del color de los píxeles.

3.1.1. Identificador del formato

Los dos primeros bytes identifican el fichero como BMP y contienen siempre el valor hexadecimal 42, 4D (66 77 en decimal, y BM en Ascii).

3.1.2. Tamaño del fichero

El tamaño del fichero se localiza en los siguientes 4 bytes pero al contrario de los números decimales, el byte más significativo en una palabra es el de la derecha (el 4º) y el menos significativo el de la izquierda (por el standard llamado *litle endian*). Por ejemplo, el tamaño de un fichero de un total de 1258 bytes se almacenaría de la siguiente manera: 234-4-0-0. El valor decimal de la palabra de cuatro octetos se calcula así: 234*1+4*256+0+0=1258.

3.1.3. Píxeles de ancho y alto

El número de columnas del mapa de bits se almacena en otra palabra de 4 bytes a partir de la posición 18 y el número de filas en otros cuatro bytes a partir de la posición 22 de manera idéntica al tamaño del fichero.

3.1.4. Paleta de colores

Ya hemos comentado más arriba que BMP de 8 bits es un formato de color indexado. La paleta de colores se almacena en la cabecera a partir de la posición 54. Cada color se codifica con sus componentes RGB pero como forman parte de la misma palabra aparecerán, al seguir el standard *little endian*, en el primer byte el azul, luego el verde y por último el rojo (BGR). Después de cada tres bytes RGB se deja otro byte con el valor cero (relleno de la palabra) de modo que la paleta ocupará 256*4=1024 bytes.

La paleta puede tener cualquier combinación de colores o una gama completa de grises (con lo que se obtendría una imagen en blanco y negro) pero cada uno de ellos, sea color o gris, se expresa con sus componentes RGB.

3.2. Información de cada píxel

El píxel de la esquina inferior izquierda es el primero en almacenarse y lo hace en la posición 1078. Este byte no almacena información de color sino el ordinal del color de la paleta (8 bits, 256 valores; uno por cada color de la paleta). El segundo píxel será el de la derecha, y así sucesivamente hasta terminar la primera fila (la fila inferior del mapa de bits). Una vez completada la fila, el siguiente byte codifica el píxel de la izquierda de la penúltima fila.

Pixel inferior izquierdo

Byte	***hex***	***Dec***	
1078	0A	10	décimo color de la paleta

Como cada palabra es de cuatro bytes, en aquellos mapas que tengan un número de columnas que no es múltiplo de 4, se completará la última palabra de la fila con bytes de relleno (lo que constituye información basura).

4. Un algoritmo de ocultación

Existen diferentes maneras de ocultar información en imágenes. A continuación mencionamos las más conocidas:
· Inserción de información en el bit menos significativo (LSB).
· Filtrado y enmascaramiento.
· Transformaciones y algoritmos

La inserción de información en el bit menos significativo es la elección que hemos utilizado para nuestra aplicación. Consiste en guardar información en los bits menos significativos de manera que los cambios, no sean percibidos por el ojo humano.

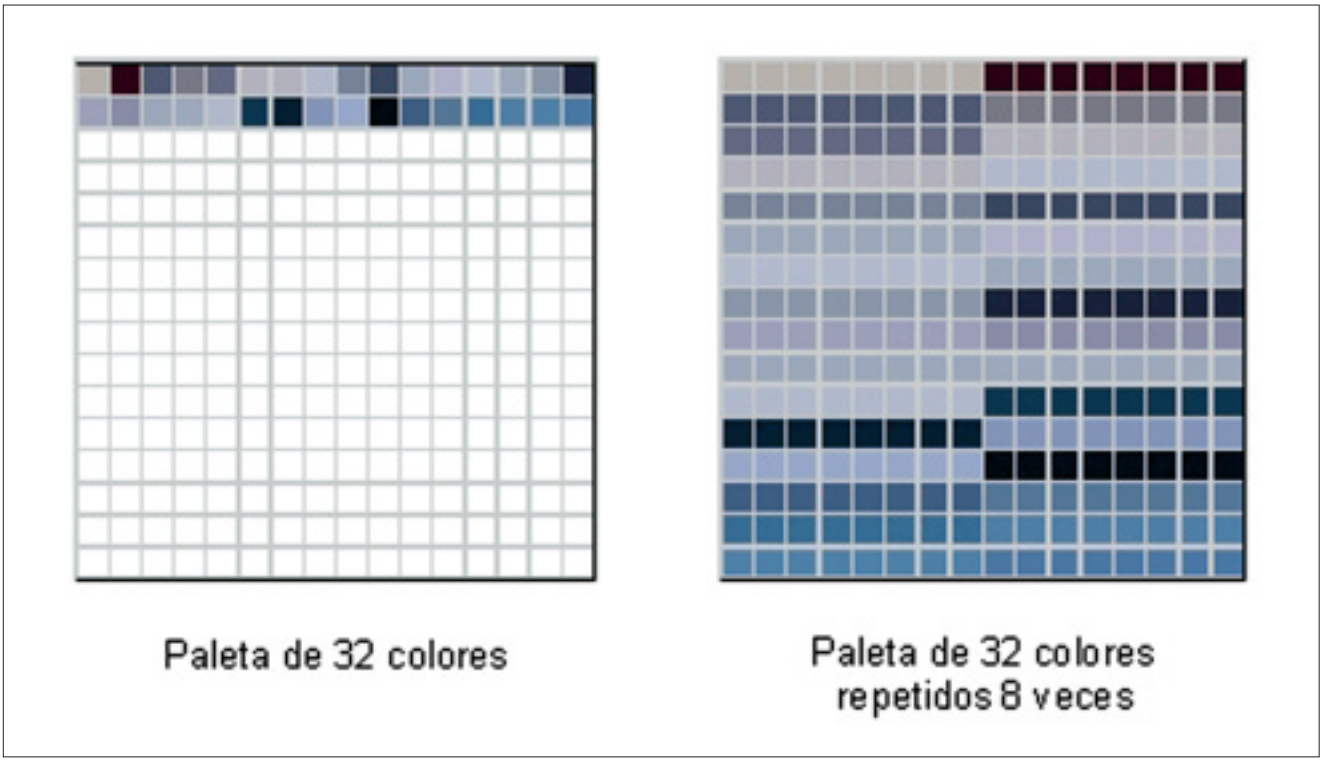


Figura 1. Paletas empleadas

Una manera de evitar esta pérdida de calidad en la imagen es utilizar una imagen modificada (como veremos a continuación) de manera que la información que, de otra manera se perdería, permanezca inamovible. En nuestro caso, las técnicas de filtrado y enmascaramiento están restringidas a imágenes de 24-bits y escala de grises.

Podemos ocultar información en la imagen aplicando una serie de modificaciones tales como la transformada de Fourier, la codificación de patrón redundante o la encriptación de la información que se ha ocultado [6].

La técnica LSB es la técnica más rápida y sencilla de esconder información. No es recomendable usarla con formatos de imagen que tengan compresión con pérdida de información. Ese es el motivo de que hayamos elegido el formato BMP para nuestra aplicación.

Para nuestra aplicación de esteganografía utilizaremos dos imágenes:

· Imagen 1 (visible): el formato de la imagen es un BMP indexado de 32 colores. La diferencia de calidad entre una imagen de 32 colores y una imagen de 256 es apenas

Figura 2. Imagen visible

Figura 3. Imagen a ocultar.

perceptible a simple vista.

· Imagen 2 (oculta): el formato de la imagen es un BMP indexado de 8 colores. Nos limitaremos a imágenes de en blanco y negro para tener una calidad razonable.

4.1. Proceso de ocultación de una imagen en otra

Para ocultar la imagen de 8 colores, lo primero que debemos hacer es transformar la imagen de 256 colores a otra imagen que solo tiene 32 colores pero cada color esta repetido 8 veces (**figura 1**).

Con esta transformación conseguimos liberar espacio en la imagen visible de tal forma que la imagen oculta, tenga cabida en el fichero de la imagen visible. En el mapa de bits de la imagen visible, modificamos la información correspondiente a un píxel, para que apunte a la primera posición (del grupo de 8 del mismo color).

De este modo, podemos almacenar la información del mapa de bits de la imagen oculta, en los 3 bit menos significativos, sin que ello, afecte al color del píxel que estemos modificando.

Si nuestro apuntador[1] es 16, significa que está apuntando al tercer color en la segunda fila y primera columna . El color 16 en binario es 00010000, aunque modifiquemos los 3 últimos bits, el color al que apuntamos no variará. Si tenemos 00010111 (23 en decimal), nuestro apuntador se moverá hasta la columna 8 de la misma fila, pero no variará su color.

Estos 3 bits últimos son los que usaremos para almacenar el *bitmap* de la imagen oculta. Para ello, simplemente debemos sumar el valor del apuntador de la imagen oculta a la imagen visible. A la vista del usuario la imagen no habrá variado, pero de esta manera, ya tenemos almacenado en la imagen visible, la información correspondiente al mapa de bits de la imagen oculta.

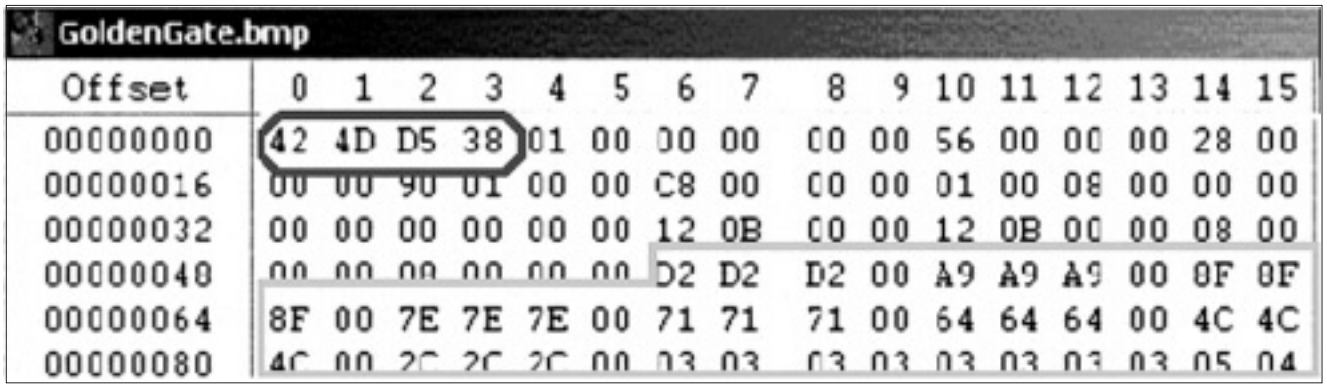
A continuación presentamos la estructura de las dos imágenes, la visible (**figura 2**) y la imagen que vamos a ocultar (**figura 3**). En este ejemplo, tenemos la imagen de un velero y dentro de ella vamos a ocultar una imagen del Golden Gate. El resultado es la imagen del velero sin ninguna modificación aparente (no la reproducimos ya que es idéntica al ojo humano que la imagen de la **figura 2**).

Ahora nos queda por almacenar la información de cabecera y la paleta de colores de la imagen a ocultar. Esta información la vamos a guardar en el 4º byte de la paleta de colores de la imagen original. Esto es posible, gracias a que en el formato

Velero.bmp

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	42	4D	35	39	01	00	00	00	00	00	B6	00	00	00	28	00
00000016	00	00	90	01	00	00	C8	00	00	00	01	00	08	00	00	00
00000032	00	00	00	00	00	00	C0	1E	00	00	C0	1E	00	00	20	00
00000048	00	00	20	00	00	00	B7	E5	C4	00	28	20	54	00	7A	6B
00000064	74	00	95	87	8F	00	8A	7B	83	00	C6	B9	C0	00	C5	B5
00000080	BC	00	CD	BD	C3	00	A0	91	96	00	6C	58	5E	00	BF	AE

Figura 4. Código hexadecimal de la imagen visible.


GoldenGate.bmp

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	42	4D	D5	38	01	00	00	00	C0	00	56	00	00	00	28	00
00000016	00	00	90	01	00	00	C8	00	C0	00	01	00	08	00	00	00
00000032	00	00	00	00	00	00	12	0B	C0	00	12	0B	00	00	08	00
00000048	00	00	00	00	00	00	D2	D2	D2	00	A9	A9	A9	00	0F	0F
00000064	8F	00	7E	7E	7E	00	71	71	71	00	64	64	64	00	4C	4C
00000080	4C	00	2C	2C	2C	00	03	03	03	03	03	03	03	03	05	04

Figura 5. Código hexadecimal de la imagen a ocultar.

BMP, la paleta de colores sólo utiliza los tres primeros bytes para codificar los componentes RGB de una imagen en color, y el 4º byte está vacío.

La paleta de colores empieza en el byte 54 de la imagen visible, tal como se muestra en la **figura 4**. El primer byte libre se encuentra en la posición 57, en esta posición almacenamos el primer byte la imagen a ocultar (ver **figura 5**). La siguiente posición vacía es la 61: en ella almacenaremos el segundo byte de la imagen oculta, Y así sucesivamente hasta haber almacenado toda la información de cabecera y paleta de la imagen oculta.

Como podemos observar en la **figura 6**, las posiciones 57,61,65,69,... se corresponden con los bytes vacíos en la representación de un color RGB. Ahora están ocupados por cada uno de los bytes que componen la cabecera y la paleta de colores de la imagen que queremos ocultar. En la primera parte, en color amarillo, podemos ver la cabecera de la imagen. En la segunda parte, en color verde, podemos ver el cuerpo de la imagen y cómo se van insertando los bytes (rodeados por un círculo) de la imagen oculta.

5. Algunas reflexiones sobre la Esteganografía

Aunque en este mismo artículo hemos comenzado apelando a los efectos más espectaculares y vinculados a la delincuencia (es decir, la esteganografía como medio de burlar una autoridad que no permite el paso de cierta información), sin embargo ésta técnica puede aportar soluciones a problemas habituales Así, si queremos proteger el uso no autorizado de imágenes que hemos creado o de las que disponemos los derechos de explotación, podemos usar la esteganografía (insertando una firma oculta en la imagen) para verificar el origen de una determinada foto. También permitiría incorporar comentarios o descriptores de las imágenes que se encuentran incorporados en el mismo fichero, haciendo así que la referencia de información a ficheros gráficos, sonoros, etc. sea más duradera y segura frente a pérdidas. De hecho, el uso de la esteganografía no se limita a ocultar información en imágenes, sino que pueden usarse otros orígenes de datos como un fichero de Audio WAV ó MP3 (por ejemplo, el programa Mandelstag (disponible en <http://www.arnal.es/free/cripto/estega/mandelst.htm>).

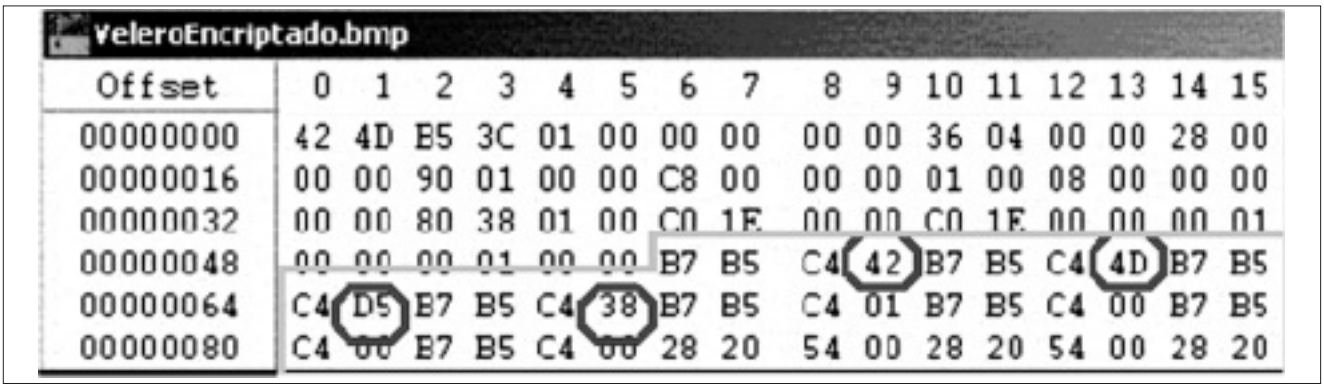
Evidentemente cuando se proporciona un medio para ocultar información, existe la corriente tecnológica contraria que trata de contrarrestar la ocultación mediante técnicas de detección conocidas como esteganálisis. Uno de los medios empleados consiste en aplicar análisis estadísticos a la codificación binaria de los ficheros para tratar de detectar patrones de repetición anormales, por ejemplo, para lo que suele ser una imagen normal. También existen otras posibilidades de sospechar la ocultación de información en un fichero y de adoptar contramedidas contra el análisis [7].

Referencias

[1] P. Pardo, «Los infinitos agujeros de la red», Expansión, 19 de septiembre de 2001 (disponible en <http://www.expansiondirecto.com/edicion/noticia/0,2458,56468,00.html>).

[2] AP, «Bin Laden's cybertrail proves elusive», USA Today, 2 de octubre de 2001 (disponible en <http://www.usatoday.com/life/cyber/tech/2001/09/20/attacks-cybertrail.htm>).

[3] AP, «150 people linked to bin Laden in custody», USA Today, 11


VeleroEncriptado.bmp

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	42	4D	B5	3C	01	00	00	00	00	00	36	04	00	00	28	00
00000016	00	00	90	01	00	00	C8	00	00	00	01	00	08	00	00	00
00000032	00	00	80	38	01	00	C0	1E	00	00	C0	1E	00	00	00	01
00000048	00	00	00	01	00	00	B7	B5	C4	42	B7	B5	C4	4D	B7	B5
00000064	C4	D5	B7	B5	C4	38	B7	B5	C4	01	B7	B5	C4	00	B7	B5
00000080	C4	00	B7	B5	C4	00	28	20	54	00	28	20	54	00	28	20

Figura 6. Código hexadecimal de la imagen oculta en la visible.

de octubre de 2001 (disponible en <http://www.usatoday.com/news/attack/2001/10/05/custody.htm>).
[4] Reuters, «Researchers: No secret bin Laden messages on sites», USA today, 3 de noviembre de 2001 (disponible en <http://www.usatoday.com/life/cyber/tech/2001/10/17/bin-laden-site.htm>).
[5] W.Wouters, «BMP format«, Clean Coding Company, 21 de febrero de 1997 (disponible en <http://www.wotsit.org/search. asp?s=windows>).
[6] N.F. Johnson, S. Jajodia, «Steganography: Seeing the Unseen», IEEE Computer, febrero, 1998, pp. 26-34.
[7] N.F. Johnson, S. Jajodia, «Steganalysis of Images Created Using Current Steganography Software», Lecture Notes in Computer Science, Vol. 1525, Springer-Verlag, 1998, pp. 273-289.

Nota

[1] Apuntador: en una imagen BMP indexada, el mapa de bits contiene un número que codifica el píxel y cuyo valor está definido en la paleta de colores que hemos definido con anterioridad. Llamamos apuntador a dicho número.

Anexo

El silencio escuda y suele encobrir
la[s] falta[s] de ingenio y *torpeza de* lenguas;
blasón que es contrario, publica sus menguas
a[l] qu*ien* mucho habla sin mucho sentir.
Como [la] hormiga que dexa de yr
holgando por tierra con la provisión,
jactóse con alas de su perdición;
lleváronla en alto, no sabe dónde yr.

El ayre gozando ageno y estraño,
rapina es ya hecha de aves que buelan;
fuerte más que ella, por cevo la llevan;
en las nuevas alas estava su daño.
Razón es que aplique a mi pluma este engaño,
no *despreciando* a los que *me* arguyen,
assí que a mí mismo mis alas destruyen,
nublosas y flacas, nascidas de ogaño.

Donde ésta gozar pensaba volando,
o yo de *screvir* cobrar más honor,
del[o] uno [y] del otro nasció disfavor;
ella es comida y a mí están cortando
reproches, revistas y tachas. Callando
obstara y los daños de invidia y murmuros;
insisto *remando*, y los puertos seguros
atrás quedan todos ya quanto más ando.

Si bien *queréys ver* mi limpio motivo,
a quál se endereça de aquestos estremos,
con qual participa, quién rige sus remos,
*A*polo, *Diana* o *Cupido* altivo,
buscad bien el fin de aquesto que escrivo,
o del principio leed su argumento;
leeldo [y] veréys que, aunque dulce cuento,
amantes, que os muestra salir de cativo.

Como el doliente que píldora amarga
o *la* rescela o no puede tragar,
métenla dentro del dulce manjar,
engáñase el gusto, la salud se alarga,
desta manera mi pluma se embarga,
imponiendo dichos lascivos, rientes,
atrae los oídos de penadas gentes,
de grado escarmientan y arrojan su carga.

***E**stando cercado* de dubdas y antojos,
compuse tal fin que principio desata;
acordé [de] dorar con oro de lata
lo más fino tíbar que vi con mis ojos,
y encima de rosas sembrar mill abrojos.
Suplico, pues suplan discretos mi falta;
teman grosseros y en obra tan alta,
o vean y callen o no den enojos.

Yo vi en Salamanca la obra presente;
movíme [a] acabarla por estas razones;
es la primera, que estó en vacaciones,
la otra, *inventarla persona prudente*,
y es la final ver la más gente
buelta y mesclada en vicios de amor;
estos amantes les pornán temor
a fiar de alcahueta ni *falso* sirviente.

Y así que esta obra *en e1 proceder*
fue tanto breve, quanto muy sutil;
vi que portava sentencias dos mill;
en forro de gracias, lavor de plazer.
No hizo Dédalo cierto a *mi ver*
alguna más prima entretalladura,
si fin diera en esta su propia escriptura
***C**ota* o *Mena con su gran Saber*.

Jamás [yo] no *vide en lengua romana,*
después que me acuerdo, ni nadie la vido,
obra de estilo tan alto y sobido
***e**n tusca ni griega ni en* castellana.
No *trae* sentencia de donde no mana
loable a su autor y eterna memoria,
al qual Jesuchristo reciba en su gloria
por su passión sancta que a todos nos sana.

Vosotros, los que amáys, tomad este enxemplo,
este fino arnés con que os defendáys;
bolved ya las riendas por que n'os perdáys;
load siempre a Dios visitando su templo.
Andad sobre aviso; no seáys dexemplo
de muertos y bivos y proprios culpados;
estando en el mundo yazéys sepultados;
muy gran dolor siento quando esto contemplo.

[**O**lvidemos los vicios que así nos prendieron;
no confiemos en vana esperança.
Temamos aquél que espinas y lança,
açotes y clavos su sangre vertieron.
La su santa faz herida escupieron;
vinagre con hiel fue su potación;
a cada santo lado consintió un ladrón.
Nos lleve, le ruego, con los que creyeron.]